(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 January 2006 (05.01.2006)

PCT

(10) International Publication Number
WO 2006/001574 A1

(51) International Patent Classification[7]: G06F 11/00

(21) International Application Number:
PCT/KR2005/000776

(22) International Filing Date: 18 March 2005 (18.03.2005)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2004-0018279 18 March 2004 (18.03.2004) KR

(71) Applicant *(for all designated States except US)*: **KOREA UNIVERSITY INDUSTRY AND ACADEMY COOPERATION FOUNDATION** [KR/KR]; 1-2 Anam-dong5-ga, Seongbuk-gu, Seoul 136-701 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CHOI, Lynn** [KR/KR]; 101-1303 Sinil Utovill Apt., Howon-dong, Uijeongbu-city, Kyungki-do 480-020 (KR). **SHIN, Yong** [KR/KR]; 662-8 Ilwon1-dong, Gangnam-gu, Seoul 135-231 (KR).

(74) Agent: **LEE, Young-Pil**; The Cheonghwa Bldg., 1571-18 Seocho-dong, Seocho-gu, Seoul 137-874 (KR).

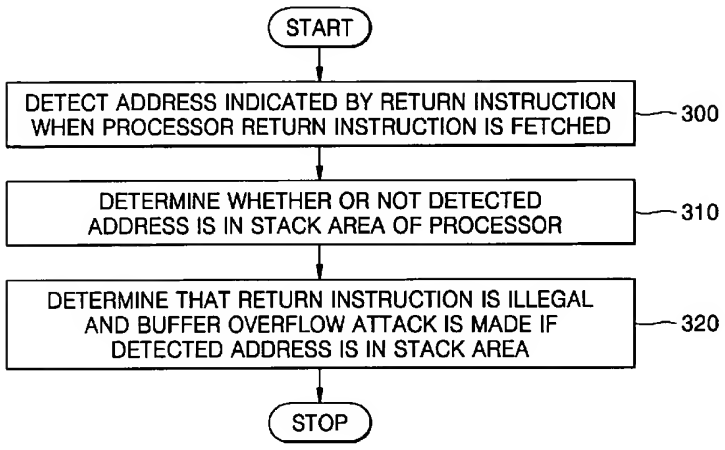
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** METHOD FOR SENSING AND RECOVERY AGATINST BUFFER OVERFLOW ATTACKS AND APPARATUS THEREOF



(57) **Abstract:** Methods and apparatuses for detecting and recovering from a buffer overflow attack are provided. A method of recovering an operation state of a processor from a buffer overflow attach includes: detecting whether a buffer overflow attack is made on any write operation while storing write operations that are potential targets of buffer overflow attacks in a predetermined location instead of an original destination to store write operations; storing the contents stored in the predetermined location at a predetermined interval in the original destination for storing write operations if no buffer overflow attack is detected and discarding unsafe write operations subsequent to a buffer overflow attack if a buffer overflow attack is detected; and ignoring the unsafe write operations subsequent to the buffer overflow attack if a buffer overflow attack is detected. Therefore, a buffer overflow attack occurring in a computer can be effectively detected, and damage of a system which is attacked can be minimized and the system can be recovered or return to the original state before the attack. A system can be effectively protected while minimizing reduction in performance of the computer system according to a method used to implement the present invention, thereby greatly improving the environments under which the computer and the Internet are used.

WO 2006/001574 A1